Client Web Services
Technical Design Document

Integrated Behavioral Health Information Systems (IBHIS) Project

---

Los Angeles County Department of Mental Health

Chief Information Office Bureau

Project Management & Administration Division

Version 1.0

09/18/2013

Disclosure Statement

This document represents the Los Angeles County Department of Mental Health's (LACDMH) technical implementation instructions for Client Web Services. This document specifies the necessary technical aspects of Client Web Services to exchange client data electronically with LACDMH. This Technical Design Document is not intended to convey information that in any way exceeds the requirements or usages of data expressed in the LACDMH Client Web Services Companion Guide. LACDMH reserves the right to modify and change the document at any time. LACDMH will disseminate the information in a timely manner, should there be any change to this document.

DOCUMENT REVISION HISTORY

Version	Release Date	Revised by	Comments/ Indicate Sections Revised
DRAFT	08/23/2013	LACDMH Integration Team	Draft version of the Technical Design Document
V1.0	09/18/2013	LACDMH Integration Team	Sections' details and diagrams have been included. Updates are made based on feedback from reviewers.

Table of Contents

A. INTRODUCTION

A.1. Purpose

The purpose of this document is to outline the technical design of the Client Web Services of LACDMH, and serve as a basic technical manual to help interpret and use the various Client Web Services operation(s). It is intended to help users gain insight into the functionality of LACDMH's Client Web Services, while also providing technicians a mechanism to communicate the technical design to their respective teams.

The design, as outlined in this document, builds upon the logical view of the Client Web Services as presented in LACDMH's Client Web Services Companion Guide, and maps those business functions to technical operations. This document helps inform the target audience about the technology and the information pertaining to the communication protocol and error handling, which in turn provides a better understanding of the product and prevents customer errors.

A.2. Background

LACDMH has a large number of Contract Providers (CPs) serving Los Angeles County clients. Currently, staff from each of these providers directly access LACDMH's Integrated System (IS) environment to enter all the data necessary for establishing and updating client information. CPs with their respective Electronic Health Record (EHR) vendors will participate in this provider integration effort with LACDMH. By leveraging Client Web Services functionality, CPs will be able to enter client data into their own respective systems. Subsequently, their systems will be able to forward these messages to IBHIS; thus, reducing the need for dual data entry.

A.3. Overview

To enable the data exchange between CPs' EHR system(s) and IBHIS, LACDMH has provided the link to the WSDL for reference. By consuming the Client Web Services, CPs will be able to call various technical operations to retrieve and commit the following information from/into IBHIS:

- Establish clients with LACDMH from their respective systems
- Establish Admission and Diagnosis of client(s)
- Get and Update client demographic information
- Create and maintain client's Financial Eligibility information for billing purposes
- Submit Client and Service Information (CSI) for California mandated State reporting
- Discharge clients
- Get Client Service History and Legacy Service History information
- Get Public Guardian and Department of Children and Family Services (DCFS) Service History information

The metadata context of the message will contain the acknowledgement, error code, and error description. During the message (request and response) exchange, acknowledgements will be sent to notify whether the requests were successfully received or not. A positive acknowledgement (ACK) will be sent for transactions without errors that adhere to the business rules published in the Companion Guide. Error codes and descriptions will not be sent for positive transaction(s). Conversely, for

transactions with errors, a negative acknowledgement (NAK) will be sent in response messages along with corresponding error codes and descriptions.

LACDMH's Client Web Services are designed to be interoperable, and are based on the W3C web services specifications for SOAP, WSDL and XML. These are also architected to provide secure access for CPs to submit and request information from LACDMH's IBHIS. Client Web Services will provide the transport layer security via a Secure Socket Layer (SSL). A high-level diagram of the architecture is shown in Figure 1.

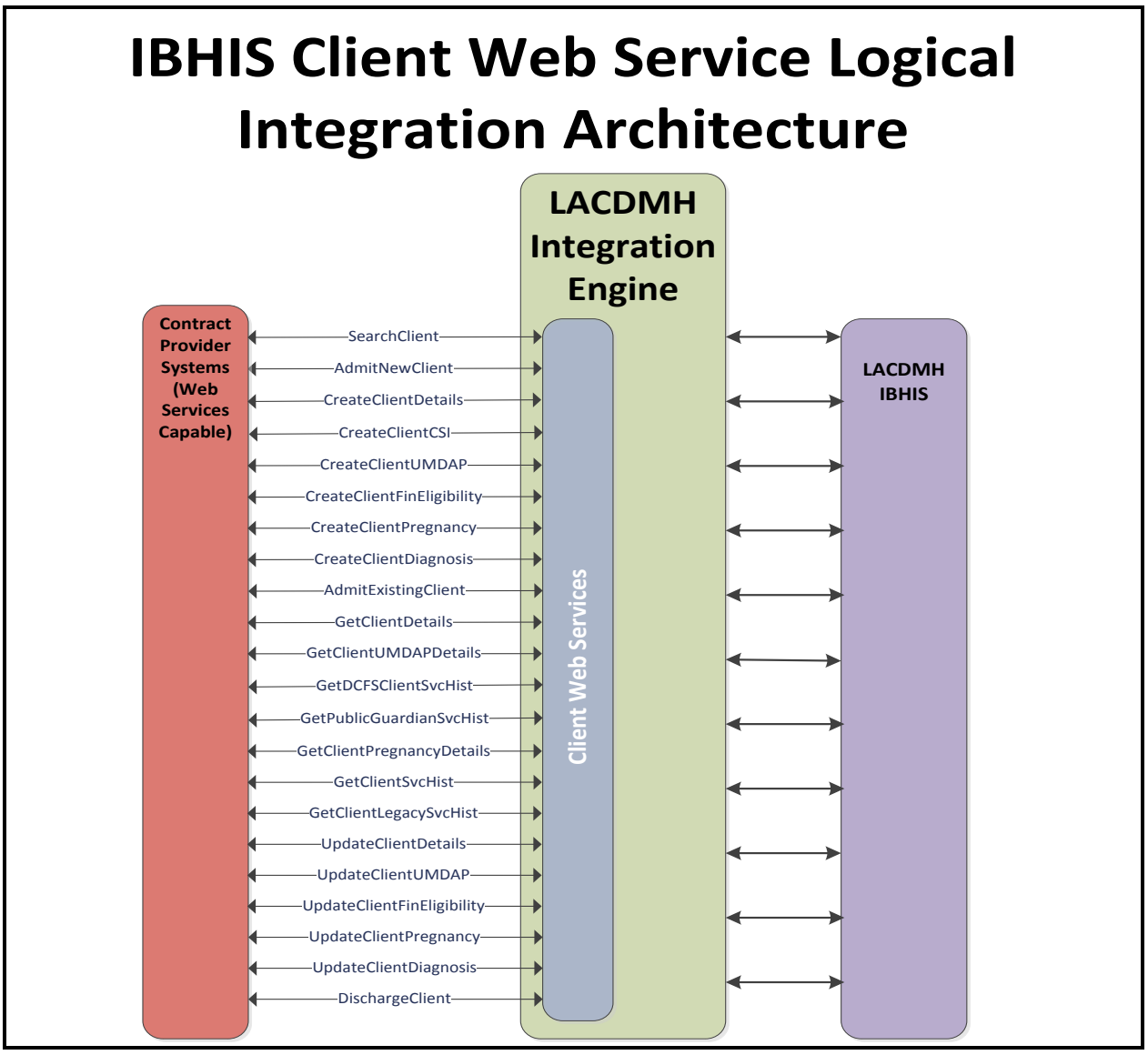

Figure 1: IBHIS Client Web Service Logical Integration Architecture

B. MAPPING – BUSINESS FUNCTIONS CALLS to TECHNICAL OPERATIONS

These operations are available for consumption in a manner which is suitable to the business needs of the CPs. The first column represents the business functions. The next column denotes the corresponding operations. The recommended sequence represents the recommended order in which the operations should be executed. Deviation from this recommended sequence may result in errors. Please refer to Section E.2 Error Codes and Descriptions for a complete listing of error codes and descriptions. If there is no value in the Recommended Sequence column, it reflects that the sequence is at the discretion of the calling party. The cardinality depicted is in relation to an operation and its results when called. The last column provides a description of the web operations.

Business Function	Web Service Operation Name	Recommended Sequence	Cardinality	Description
Search Client	SearchClient	0	1…*	Provides ability to search clients based on the submitted parameters for Client information.
Create and Admit New Client	AdmitNewClient	1	1...1	Provides ability to create a client and submit an admission for a new client.
	CreateClientCSI	2	1...1	Provides ability to submit State mandated Client Service Index (CSI) Data for a specific client.
	CreateClientUMDAP	3	1...1	Provides the ability to submit “Uniform Method of Determining Ability to Pay” (UMDAP) data for a specific client.
	CreateClientFinEligibility	4	1...1	Provides the ability to submit financial eligibility data for a specific client. **NOTE**: The capturing and accuracy of this data is essential for successful claims processing.
	CreateClientPregnancy	5	0...1	If a client is **female**, this operation provides the ability to submit pregnancy related data for a specific client. This operation is **conditional**.
	CreateClientDiagnosis	6	0...1	Provides ability to submit a new diagnosis for a specific client. This operation is not required at the time of creating the client.

Business Function	Web Service Operation Name	Recommended Sequence	Cardinality	Description
Admit Existing Client	AdmitExistingClient	1	1...1	Provides ability to submit an admission for a specific client.
Update Client	UpdateClientDetails		1...1	Provides ability to update the detailed client demographic and CSI data for a specific client.
	UpdateClientUMDAP		1...1	Provides the ability to update "Uniform Method of Determining Ability to Pay" (UMDAP) data for a specific client.
	UpdateClientFinEligiblity		1...1	Provides the ability to update existing financial eligibility data for a specific client. **NOTE**: The capturing and accuracy of this data is essential for successful claims processing.
	UpdateClientPregnancy		1...1	If a client is **female**, this operation provides the ability to update pregnancy related data for a specific client.
	UpdateClientDiagnosis		1...1	Provides ability to update an existing diagnosis for a specific client.
Discharge Client	DischargeClient		1...1	Provides the ability to submit a discharge for a specific client.
Get Client Information	GetClientDetails		1...1	Provides ability to retrieve detailed client demographic and CSI data for a specific client.
	GetClientUMDAPDetails		1...*	Provides the ability to retrieve "Uniform Method of Determining Ability to Pay" (UMDAP) data for a specific client.
	GetPublicGuardianSvcHist		0...*	Provides the ability to retrieve client's Public Guardian history.

Business Function	Web Service Operation Name	Recommended Sequence	Cardinality	Description
	GetDCFSClientSvcHist		0…*	Provides the ability to retrieve client's DCFS service history.
	GetClientPregnancyDetails		0…*	If a client is female, this operation provides the ability to retrieve pregnancy related data for a specific client, if it exists.
Get Client Treatment History	GetClientSvcHist		1…*	Provides ability to retrieve service history details of a client grouped by program of service.
	GetClientLegacySvcHist		1…*	Provides ability to retrieve Client legacy Integrated System (IS) service history details
Other	CreateClientDetails		1..1	Provides ability to submit detailed client demographic and CSI data.

C. RECOMMENDED OPERATION FLOW

C.1 Create and Admit New & Existing Client

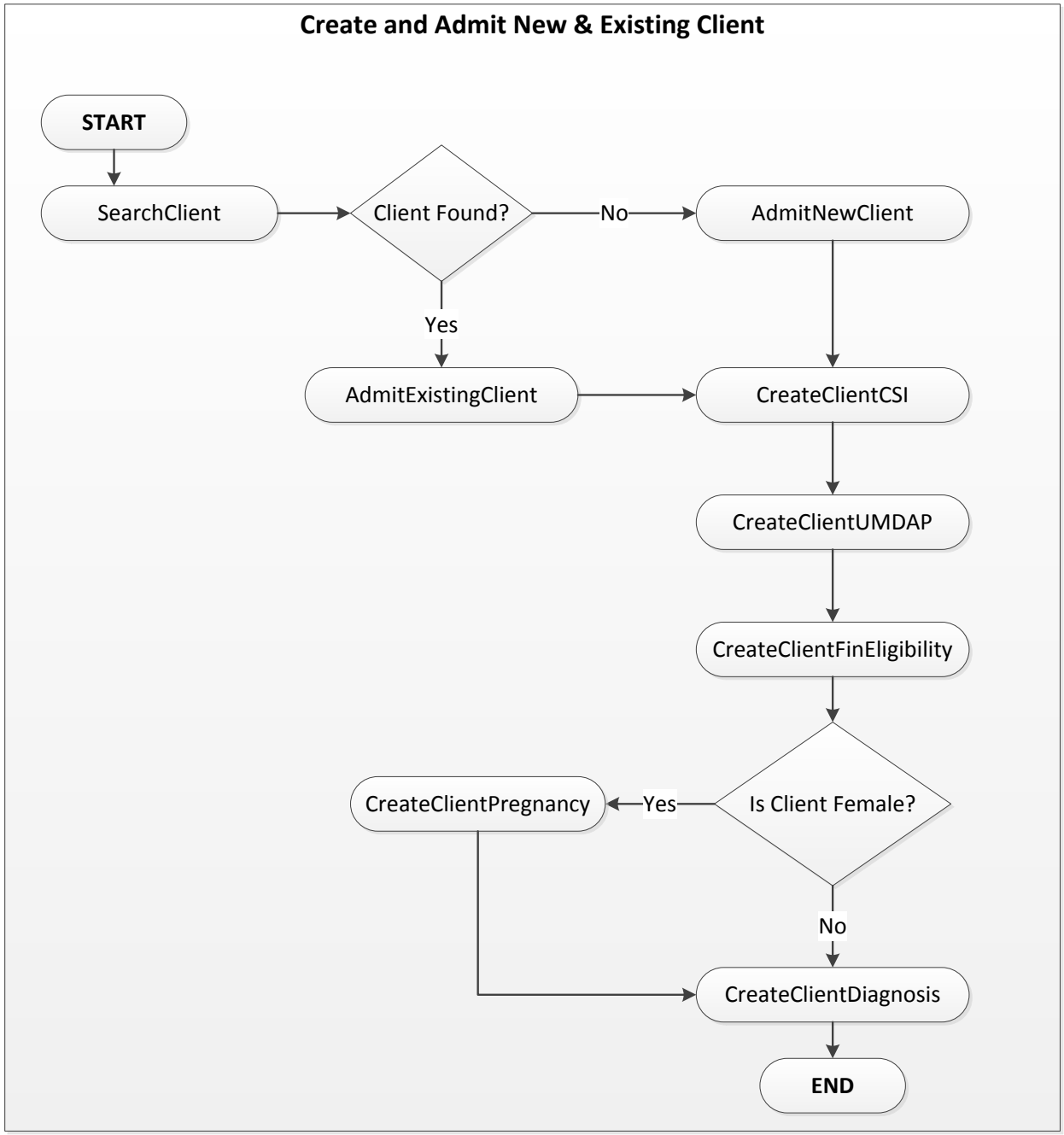

Figure 2: Create and Admit New & Existing Client Workflow

C.2 Update Client

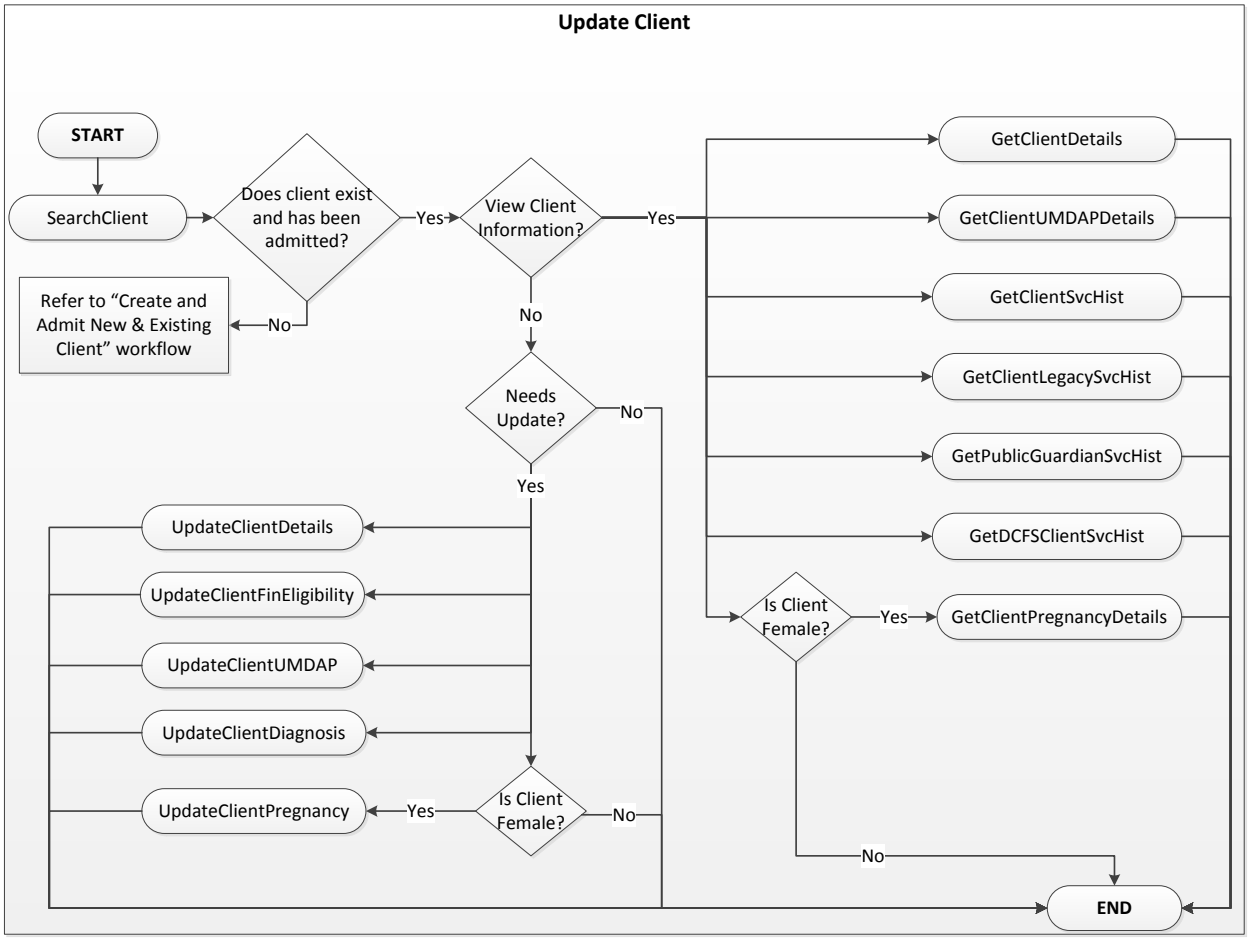

Figure 3: Update Client Workflow

C.3 Discharge Client

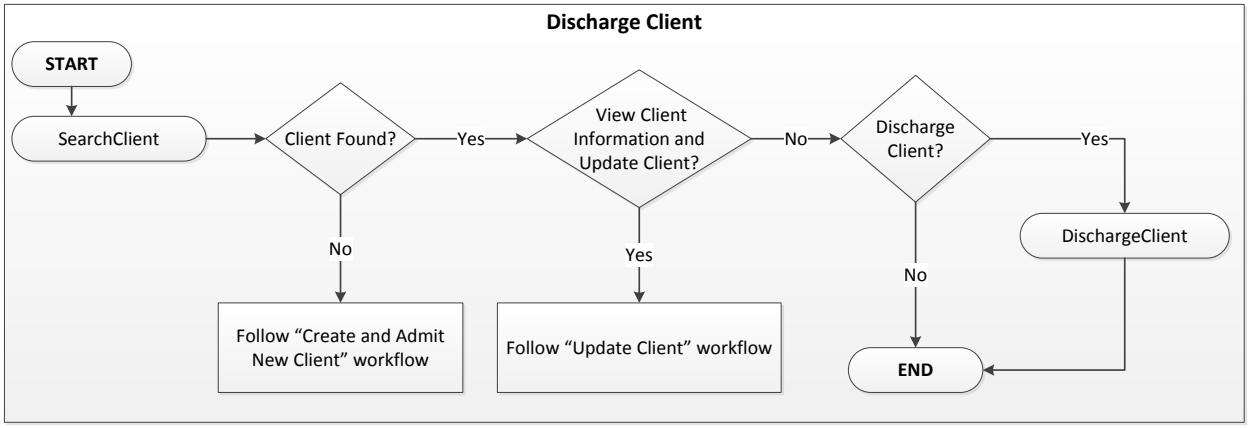

Figure 4: Discharge Client Workflow

D. SECURITY

D.1 Authorization & Authentication

The Client Web Services uses X.509 Digital Certificates and a Managed Public Key Infrastructure (MPKI) to authenticate and authorize calling parties. To access Web Services successfully, callers **must** provide a Program Identifier (previously referred to as the Legal Entity Number) along with their LACDMH assigned Digital Certificate. To illustrate placement of the certificate thumbprint and Program Identifier, the sample SOAP messages are provided below using Search Client Input and Output operations:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://b2b.dmh.lacounty.gov/ews/EstablishClient/2013-0701"
xmlns:lac="http://b2b.dmh.lacounty.gov/ews/EstablishClient/2013-0701/MessageContext">
 <soapenv:Header>
  <Certificate>
   B74E1D8C6135547B59EE846D030A5CAAAD8E6B5Z
  </Certificate>
</soapenv:Header >
  <soapenv:Body>
   <ns:SearchClient_Input>
    <lac:MessageContextInput ProgramID="?"/>
     <Client ClientID="?" FirstName="?" LastName="?" DateOfBirth="?" SocialSecurityNumber="?"
MediCalPolicyNumber="?" Gender="?"/>
   </ns:SearchClient_Input>
  </soapenv:Body>
</soapenv:Envelope>
```

Figure 5: Search Client Input - Sample SOAP Message

Please note that the certificate thumbprint is expected in the SOAP Header. In the Message Context Input of the request, “ProgramID” is required (Figure 5). However, in the response message, an Acknowledgement and Error is provided in the Message Context Output property (Figure 6).

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://b2b.dmh.lacounty.gov/ews/EstablishClient/2013-0701"
xmlns:lac="http://b2b.dmh.lacounty.gov/ews/EstablishClient/2013-0701/MessageContext">
 <soapenv:Header>
  <Certificate>
   B74E1D8C6135547B59EE846D030A5CAAAD8E6B5Z
  </Certificate>
</soapenv:Header >
  <soapenv:Body>
   <ns:SearchClient_Output>
    <lac:MessageContextOutput Error="?" Acknowledgement=""/>
     <Client ClientID="?" ClientName="?" DateOfBirth="?" AddressStreet="?" AddressCity="?"
AddressState="?" Alias="" Score=""/>
   </ns:SearchClient_Output>
  </soapenv:Body>
</soapenv:Envelope>
```

Figure 6: Search Client Output - Sample SOAP Message

In addition to the message layout, the authentication process is as follows (Figure 7):

- (1) CP initiates a call, requesting LACDMH resource(s).
- (2) Subsequent to that request, a certificate exchange will occur - DMH will present a certificate, identifying itself to the caller.
- (4) The caller will present a X.509 certificate thumbprint identifying itself to DMH.
- (3&5) Each party confirms the exchanged certificates by an independent Certificate Authority.
- (6) Once confirmation has taken place, access to the requested resource(s) is granted.

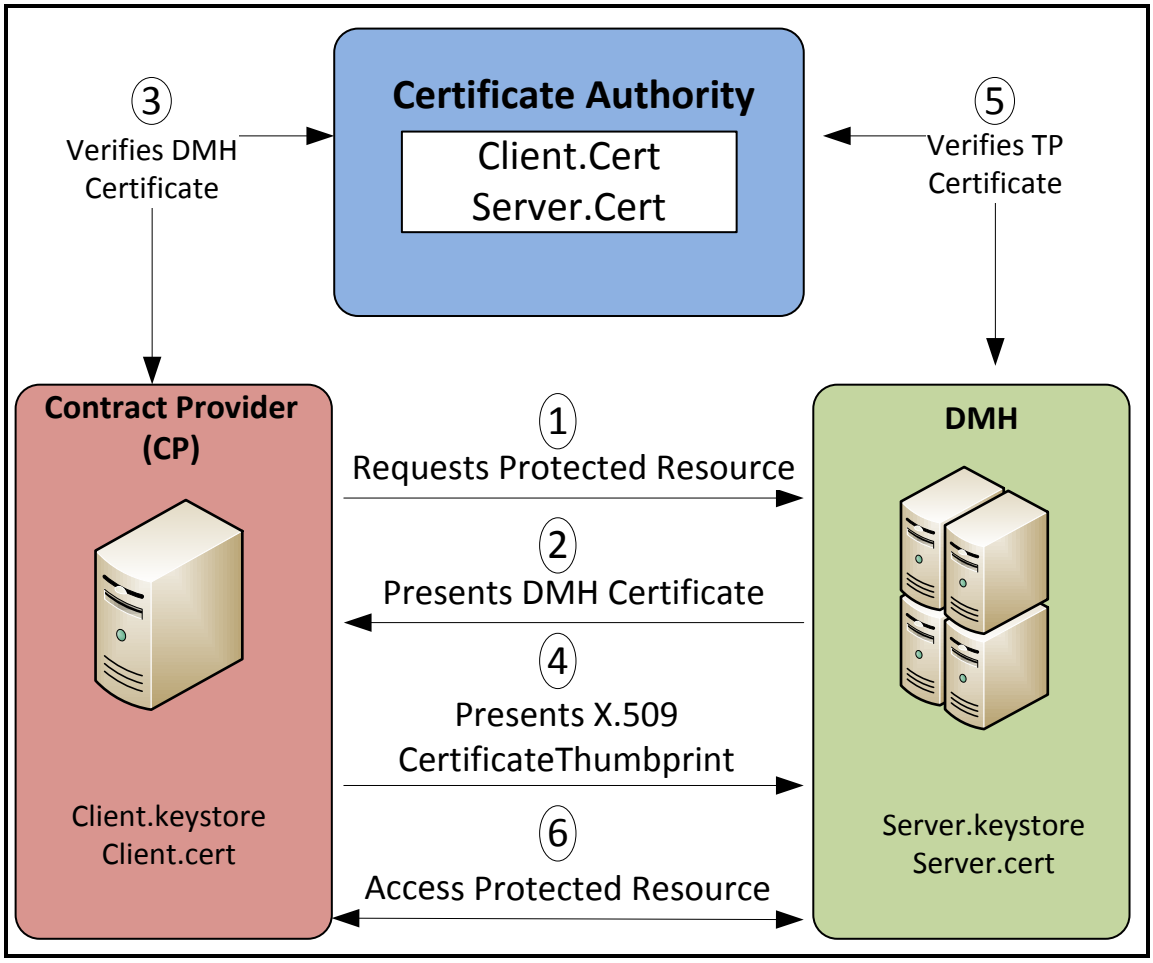

Figure 7: Authentication Process

E. APPENDIX

E.1 Location of WSDLs

LACDMH IBHIS Client Web Services - WSDL can be found in the LACDMH IBHIS EDI website from the following URL (Click on the link).

WSDL Location URL:
http://lacdmh.lacounty.gov/hipaa/documents/b2b.dmh.lacounty.gov.ews.EstablishClient.2013-0701.wsdl

Please refer to the **LACDMH Client Web Services Companion Guide** for information regarding data elements. This guide can be found at the following URL (Click on the link).

LACDMH Client Web Services Companion Guide Location URL:
http://lacdmh.lacounty.gov/hipaa/IBHIS_EDI_Guides.htm

E.2 Error Codes and Descriptions

To assist with exception handling, DMH has provided a detailed list of error codes with descriptions.

Please download **LACDMH Client Web Services Error Codes and Descriptions version 1** file from the DMH IBHIS EDI website (Click on the link).

Error Codes File Location URL:
http://lacdmh.lacounty.gov/hipaa/documents/LACDMH_ClientWebServicesErrorCodesAndDescriptions_v1.pdf

E.3 Definition of Terms

ACK: The abbreviation for Acknowledgement. A positive acknowledgment confirms receipt of data.

Certificate Authority (CA): CA is an entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

CP (Contract Provider): These are the mental health service entities contracted with LACDMH to provide care to LACDMH mental health clients.

CSI (Client and Service Information): This is a set of data required by the State of California's Department of Health Care Services (DHCS). Data must be provided monthly by all county mental health programs and summarized at the state level. The system began in 1998 and is the successor to the Client Data System (CDS). The system is used to provide service and utilization data to DHCS's management and staff, county mental health programs, other federal and state agencies, the Legislature, and other interested groups and individuals

EDI (Electronic Data Interchange): Data exchange standard from the National Institute of Standards and Technology that involves computer-to-computer interchange of strictly formatted messages that represent documents. EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient. It distinguishes mere electronic communication or data exchange, specifying that "in EDI", the usual processing of sent and received messages is by computer only.

EHR (Electronic Health Record): EHR is a patient record in digital format that is entered, stored and maintained by computerized information systems. It is designed to capture and represent data that accurately capture the state of the patient at all times. It allows for an entire patient history to be viewed without the need to track down the patient's previous paper-based medical record volume and assists in ensuring data is accurate, appropriate and legible. EHRs may include a range of data, including but not limited to demographics, medical history, medications and allergies and laboratory test results.

LACDMH (Los Angeles County Department of Mental Health): It is the largest County mental health department in the United States providing mental health services for Los Angeles County residents. LACDMH directly operates 75 program sites in the County and serves over 250,000 clients annually.

MPKI (Managed Public Key Infrastructure): It is the infrastructure, which LACDMH uses to create, manage, distribute, use, store, and revoke digital certificates.

NAK: The abbreviation for Negative Acknowledgement. A negative acknowledgment confirms that no data was received.

SOAP (Simple Object Access Protocol): It is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment, using XML technologies.

SSL (Secure Sockets Layer): It is a cryptographic protocol that is designed to provide communication security over the Internet. SSL uses X.509 certificates and asymmetric cryptography to assure the counterparty with whom they are talking, and to exchange a symmetric key.

W3C (World Wide Web Consortium): W3C is an international community that develops open standards to ensure the long-term growth of the Web and associated technologies. For more information see www.w3.org

WSDL (Web Services Description Language): It is an XML-based interface description language that is used for describing the functionality offered by a web service. A WSDL description of a web service

provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns.

X.509 Digital Certificate: In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

XML (Extensible Markup Language): XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

|End of the Document|